REMARKS/ARGUMENTS

Claims 1-31 are pending, claims 1, 2, 4, 10-18 were amended. Claims 1-31 remain pending.

The Specification was amended to correct various and formalities, as suggested by the Examiner. In response to claim objections, claims 2 and 11 were amended to delete the second occurrence of the word "and" -- no such repetition of the word "and" was found in claim 20, and claims 10-18 were amended to replace "media" with "medium."

Independent claims 1, 11 and 28 were amended similar to the recitations of independent claim 19 to make clear that the recited limitations are performed by the indicia generating devices. In addition, independent claims 1, 11, and 19 were amended to make clear that the indicia generating devices are divided into groups based on geographic designations, and that sets of verifications keys are encrypted as a function of one of the geographic destinations and assigned to a corresponding indicia generating device group. Support for the amendment can be found throughout the specification and original claims. Accordingly no new matter has been entered.

A telephone interview was held on June 1, 2004, between Examiner Colin and Attorney for Applicant. Attorney for Applicant thanks and appreciates the helpful comments and suggestions offered by Examiner Colin to facilitate allowance of the application. In the interview, the differences between Gravell (US 6,546,377) and the amended claims were discussed. Namely, even if a digital token is considered analogous to the recited verification keys, Gravell still fails to teach dividing both the generating devices and verification keys and key IDs into groups based on geographic designation and distributing only the verification keys and key IDs for each group to the corresponding generating devices. In addition it was discussed

that with reference to amended claim 1, the amended independent claims now make it clear that steps (a)-(c) are performed by the generating devices, whereas in Gravel, step (c) is performed by the data center, while steps (a) and (b) are missing from Gravell since all of Gravell's keys are stored in the data center and not transmitted to the mailers' PCs for receipt.

The Examiner rejected claims 1, 7, 10, 16, 19, and 25 under 35 USC §102 (e) as being anticipated by US patent 6,546,3772 Gravell et al. The Examiner rejected claims 2-3, 5-6, 8-9, 11-12, 14-15, 17-18, 20-21, 23-24, 26-31 under 35 USC §103 (a) as being unpatentable over Gravell in view of US patent 6, 29 5,359 to Cordery et al. The Examiner rejected claims 4, 13 and 22 under 35 USC §103(a) as being unpatentable over Gravell in view of Cordery and further in view of US patent 6,005,945 to Whitehouse. Applicant respectfully disagrees.

The present invention is related to using cryptographic methods, such as asymmetric public-key cryptography, to prevent counterfeiting of the USPS information printed onto mail pieces and other items. The present invention accomplishes this by securely distributing verification keys and key IDs to indicia generating devices.

Gravell's system is similar to the prior art discussed in the background of the invention in the present application in which all keys for the generating postage are stored at the postage verifier. Gravell explicitly states "all mailer information, including **use of public or private keys, is accessed from a Database Server** 36 where the mailer information is securely stored using secure cryptographic processes and protocols" (col. 7, lines 27-37). As described in the background of the present invention, maintaining possession of the entire set of cryptographic keys used by the postage generating devices at the postage verifier is disadvantageous. The postage verifier a single point of attack: if the verifier is broken into, a perpetrator may easily impersonate all postage generating devices in the postal system (Page 3, line 21+).

The present invention solves this problem by dividing postage generating devices (PDGs) into n groups corresponding to different geographic designations, and by assigning a set of set of verification keys, V_i, to each PGD group, where each verification key in the set is encrypted as a function of one the corresponding destination region.

Steps (a) and (b) in amended claim 1 now recites that a set of verification keys and corresponding key ID's are encrypted as a function of one of the same geographic designation as the PDG's to which the keys are assigned. In Gravell, there is no teaching or suggestion that any type of keys are grouped based on geographic designation and then assigned to corresponding groups of local print systems. The Examiner cites Gravell col. 4, lines 66 through col. 5, line 12 for teaching a plurality of PGDs that have been divided into n groups identified by group designation. However, the cited passage merely describes the virtual postage metering system has postage metering accounts associated with each mailer.

The Examiner also considers Gravell's PSA's to meet the recitation of key ID's. However, a PSA is a postage meeting account associated with each licensed mailer (column 5, lines 1-2). Thus, a PSA is neither associated with a verification key nor is encrypted as a function of the same geographic designation used to encrypt the corresponding verification key, as the key IDs recited in claim 1.

The amended independent claims also make it clear that the "receiving" of the keys in steps (a) and (b) is performed by the generating devices. As stated above, in Gravell, all keys are maintained at the data center and not passed out to the mailer's local print systems.

Step (c) of claim 1, in which the indicium is generated and evidenced, is also performed by the generating devices. In Gravell, by contrast, the evidencing is performed by the data center. As stated above, performing the evidencing at the data center is insecure, as a hacker

could obtain all the keys from one location. In the present invention, the verification keys are split up and sent to respective device groups so that if one device is comprised, the hacker would only obtain a subset of the verification keys, a would still need to crack the identification keys to determine which verification key to use. Gravell, alone or in combination, simply fails to tech or suggest such functionality. Independent claims 11, 19 and 28 include similar recitations.

Based on the foregoing, it respectfully submitted that Gravell fails to teach or suggest independent claims 1, 11, 19, and 28, even when combined with the secondary references.

It is respectfully submitted that a secondary reference stands or falls with a primary reference, and the secondary references fail to make up for the lack of teaching in Gravell. In view of the foregoing, it is submitted that claims 1-31 are allowable over the cited references. Because the secondary references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-31 as now presented.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

June 9, 2004
Date

Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540